E-FILED
Tuesday, 15 October, 2019 12:23:27 PM
Clerk, U.S. District Court, ILCD

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS

NOREEN PERDUE and DUSTIN MURRAY, individually and on behalf of all others similarly situated,	)	CASE NO.
Plaintiffs,	)	**CLASS ACTION COMPLAINT**
v.	)	
HY-VEE, INC.,	)	
Defendant.	)	**JURY TRIAL DEMANDED**

Plaintiffs Noreen Perdue and Dustin Murray ("Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Defendant Hy-Vee, Inc. ("Hy-Vee" or "Defendant") based on personal knowledge as to their own experiences and upon information and belief on investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated whose personal and non-public information, including credit card and debit card numbers, expiration dates, cardholder names, and other card information (collectively, "Card Information") was compromised in a massive security breach of Hy-Vee's computer servers (the "Data Breach").

2. As a result of the Data Breach, millions of consumers have reportedly had their sensitive credit and debit card information exposed to fraudsters resulting from purchases made at Hy-Vee's gas pumps, restaurants, and its drive-through coffee shops.

3. In an initial Notice of Payment Card Data Incident (the "Notice") posted on Hy-Vee's website, the very first sentence claims that "Hy-Vee takes the security of payment card data very seriously."[1] As evidenced by the Data Breach, this cannot be true.

4. The Notice contains very little detail about the breach. In fact, Hy-Vee first posted the Notice and announced the Data Breach to the public on August 14, 2019, but for nearly two months after that announcement, it provided little detail about what happened.[2] Apparently, Hy-Vee believed it was best to wait until its internal investigation of the Data Breach concluded until providing its customers with details about the breach so they can protect against fraud and identity theft.

5. The Notice provided that "[b]ecause the investigation is in its earliest stages, we do not have any additional details to provide at this time. We will provide notification to our customers as we get further clarity about the specific timeframes and locations that may have been involved."[3]

6. Only on October 3, 2019, nearly two months after announcing the Data Breach, did Hy-Vee share additional details with consumers. In a company announcement titled "Hy-Vee Reports Findings from Investigation of Payment Card Data Incident" (the "Report"),[4] Hy-Vee provided additional information about the breach, including that the breach was detected on July 29, 2019; the window of the breach was from December 14, 2018 to July 29, 2019 for fuel

[1] HY-VEE, *Notice of Payment Card Data Incident*, available at https://www.hy-vee.com/corporate/news-events/announcements/notice-of-payment-card-data-incident/ (last visited Oct. 4, 2019). https://www.hy-vee.com/corporate/news-events/announcements/notice-of-payment-card-data-incident/ (last visited Oct. 4, 2019).
[2] "Hy-Vee explains why few details have been released in data breach," available at https://www.kcci.com/article/hy-vee-explains-why-few-details-have-been-released-in-data-breach/28854757 (last visited Oct. 4, 2019).
[3] HY-VEE, *Notice of Payment Card Data Incident*, *supra* note 1.
[4] HY-VEE, *Hy-Vee Reports Findings from Investigation of Payment Card Data Incident*, available at https://www.hy-vee.com/PaymentCardIncident/ (last visited Oct. 4, 2019).

pumps (i.e., over 7 months long), and from January 15, 2019 to July 29, 2019 for restaurants and drive-thru coffee shops (i.e., over 6 months long); that for some restaurants, the breach began as early as November 9, 2018; and that for one location, the breach continued through August 2, 2019.[5]

7. In the Report, Hy-Vee also announced that it had published a list of locations and an online tool for determining whether a given location was impacted by the Data Breach, and during what period. The Report also indicated that Hy-Vee *will be* sending out notices to those individuals who have been impacted.[6]

8. As alleged herein, Hy-Vee's failure to implement adequate data security measures for this sensitive customer information directly and proximately caused injuries to Plaintiffs and the class.

9. The Data Breach was the inevitable result of Hy-Vee's inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and despite the fact that these types of data breaches were and are occurring throughout the restaurant and retail industries, Hy-Vee failed to ensure that it maintained adequate data security measures causing customer Card Information to be stolen.

10. As a direct and proximate consequence of Hy-Vee's conduct and data security shortcomings, a massive amount of customer information was stolen from Hy-Vee and exposed to criminals. While Hy-Vee has not confirmed the exact number of cards that were compromised, according to KrebsonSecurity—a leading expert on data security—more than 5.3

[5] HY-VEE, *Hy-Vee Reports Findings from Investigation of Payment Card Data Incident*, *supra* note 4.
[6] *Id*.

million new accounts belonging to cardholders from 35 states have had their sensitive Card Information placed on the dark web for sale to fraudsters.[7] Victims of the Data Breach have had their Card Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise been injured.

11. Moreover, Plaintiffs and class members have been forced to spend significant time associated with, among other things, closing out and opening new credit or debit card accounts, ordering replacement cards, obtaining fraud monitoring services, losing access to cash flow and credit lines, monitoring credit reports and accounts, and/or other losses resulting from the unauthorized use of their cards or accounts.

12. Rather than providing meaningful assistance to consumers to help deal with the fraud that has and will continue to result from the Data Breach, Hy-Vee simply tells them to "closely monitor [their] payment card statements for unauthorized activity,"[8] shifting the onus to its customers. In contrast to what has been frequently made available to consumers in recent data breaches, Hy-Vee has not offered or provided any credit monitoring service or fraud insurance to date.

13. Plaintiffs and class members seek to recover damages caused by Hy-Vee's negligence, negligence *per se*, breach of contract, and violations of state consumer protection statutes. Additionally, Plaintiffs seek declaratory and injunctive relief as a result of the conduct of Hy-Vee discussed herein.

---

[7] KREBSONSECURITY, "Breach at Hy-Vee Supermarket Chain Tied to Sale of 5M+ Stolen Credit, Debit Cards," available at https://krebsonsecurity.com/2019/08/breach-at-hy-vee-supermarket-chain-tied-to-sale-of-5m-stolen-credit-debit-cards/ (last visited Oct. 4, 2019).

[8] HY-VEE, *Notice of Payment Card Data Incident*, *supra* note 1.

PARTIES

Plaintiff Noreen Perdue

14. Plaintiff Noreen Perdue is an adult residing in Avon, Illinois. During the period of time when the Data Breach was occurring, Ms. Perdue used her debit card to make a purchase in the amount of $40 from the Hy-Vee gas pump located in Galesburg, Illinois.

15. On August 26, 2019 Ms. Perdue received a letter from her bank, Thompkins State Bank, which notified her that her debit card had been compromised. In addition, Ms. Perdue received a phone call from her bank's fraud department which confirmed that her card was compromised in the Hy-Vee Data Breach. To date, Hy-Vee has provided no direct notice of the Data Breach to Ms. Perdue.

16. As a result, Thompkins State Bank was forced to close her debit card account and issue her a new card. Ms. Perdue went for three weeks without access to her card, which is the only way she can access her money and pay her bills. During that time, she was without access to these funds.

17. Prior to learning that her payment card was impacted by the Data Breach, Ms. Perdue had not experienced credit card fraud or identity theft with respect to that card.

18. Although Ms. Perdue was ultimately provided with a new card, as a result of having been victimized by the Data Breach, she was required to spend a significant amount of time addressing the fraud concerns related with her compromised card.

19. Had Ms. Perdue known that Hy-Vee would not adequately protect her Card Information and other sensitive information entrusted to it, she would not have made a purchase at Hy-Vee using her payment card.

20. As a result of Hy-Vee's failure to adequately safeguard Plaintiff's Card Information, Ms. Perdue has been injured.

Plaintiff Dustin Murray

21. Plaintiff Dustin Murray is an adult residing in Columbia, Missouri. Mr. Murray is a regular customer of Hy-Vee and eats at Hy-Vee's in-store restaurant approximately 2-3 times per month. Mr. Murray used his debit card multiple times at two separate Hy-Vee in-store restaurant locations in Columbia, Missouri during the breach period.

22. On September 16, 2019 Mr. Murray became aware of the Data Breach after his bank, Central Bank, sent him an email notification stating that his debit card was affected by the Data Breach. To date, Hy-Vee has provided no direct notice of the Data Breach to Mr. Murray.

23. As a result of the breach, Central Bank was forced to close Mr. Murray's debit card account and issue him a new card.

24. Although Mr. Murray's bank ultimately provided him a new card, as a result of having been victimized by the Data Breach, Mr. Murray was required to spend approximately 3 hours dealing with the side-effects of the breach.

25. Had Mr. Murray known that Hy-Vee would not adequately protect his Card Information and other sensitive information entrusted to it, he would not have made a purchase at Hy-Vee using his payment card.

26. As a result of Hy-Vee's failure to adequately safeguard Mr. Murray's Card Information, Mr. Murray has been injured.

Defendant

27. Defendant Hy-Vee, Inc. maintains its principal place of business at 5820 Westown Parkway, West Des Moines, IA 50266.

28. Hy-Vee operates as a chain of supermarket locations, fuel pumps, convenience stores, gas stations, and drive-through coffee shops.

29. According to its website, Hy-Vee owns over 240 retail stores in eight Midwestern states, including Iowa, Illinois, Kansas, Minnesota, Missouri, Nebraska, South Dakota, and Wisconsin.

30. Many Hy-Vee locations are full-service supermarkets, offering bakeries, catering, florists, dine-in and carryout food service, wine and spirits, pharmacies, health clinics, HealthMarkets (natural and organic products) and coffee kiosks. The company also maintains fuel stations with convenience stores, fitness centers, and full service restaurants at some of its properties.

31. Furthermore, Hy-Vee owns three Wahlburgers locations, including one in the Mall of America in Bloomington, Minnesota; a location in West Des Moines, Iowa; and a location in Olathe, Kansas.

JURISDICTION AND VENUE

32. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Hy-Vee. See 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

33. This Court has personal jurisdiction over Hy-Vee. Hy-Vee has sufficient minimum contacts with the state of Illinois—including the operation of numerous stores in Illinois—and intentionally avails itself of the consumers and markets within the state through the promotion, marketing, and sale of its products and services.

34. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because Hy-Vee conducts substantial business in this district. A substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this district.

FACTUAL ALLEGATIONS

The Hy-Vee Data Breach

35. On or about August 14, 2019, Hy-Vee confirmed in a "Notice of Payment Card Data Incident" alert posted on its website that it had been made aware of a possible data breach that compromised customers' sensitive Card Information. The Notice provides the following:

> Hy-Vee takes the security of payment card data very seriously. We want to make customers aware of an investigation we are conducting into a security incident involving our payment processing systems that is focused on transactions at some Hy-Vee fuel pumps, drive-thru coffee shops, and restaurants, as well as to provide information on the measures we have taken in response and steps customers may consider taking as well.
>
> After recently detecting unauthorized activity on some of our payment processing systems, we immediately began an investigation with the help of leading cybersecurity firms. We also notified federal law enforcement and the payment card networks. We believe the actions we have taken have stopped the unauthorized activity on our payment processing systems. Our investigation is focused on card transactions at our fuel pumps, drive-thru coffee shops, and restaurants (which include our Market Grilles, Market Grille Expresses and the Wahlburgers locations that Hy-Vee owns and operates). These locations have different point-of-sale systems than those located at our grocery stores, drugstores and inside our convenience stores, which utilize point-to-point encryption technology for processing payment card transactions. This encryption technology protects card data by making it unreadable. Based on our preliminary investigation, we believe payment card transactions that were swiped or inserted on these systems, which are utilized at our front-end checkout lanes, pharmacies, customer service counters, wine & spirits locations, floral departments, clinics and all other food service areas, as well as transactions processed through Aisles Online, are not involved.
>
> Because the investigation is in its earliest stages, we do not have any additional details to provide at this time. We will provide notification to our customers as we get further clarity about the specific timeframes and locations that may have been involved.

> It is always advisable to closely monitor your payment card statements for any unauthorized activity. If you see an unauthorized charge, immediately notify the financial institution that issued the card because cardholders are not generally responsible for unauthorized charges reported in a timely manner. The phone number to call is typically located on the back of the payment card.[9]

36. The Notice makes clear that at Hy-Vee's fuel pumps, drive-thru coffee shops, and restaurants (i.e., the locations impacted by the breach), it did not utilize card encryption technology. The Notice also confirms that Hy-Vee did in fact utilize encryption technology at its grocery store checkout lanes, pharmacies, and convenience stores, and does not believe these locations were impacted as they have point of sale systems that rely on security technology designed to defeat card-skimming malware.[10]

37. It is unclear why Hy-Vee decided to use point to point encryption technology inside of its grocery stores, but not for the fuel pumps, drive-thru coffee shops, and restaurant locations that were impacted by the Data Breach.

38. According to data security leader KrebsOnSecurity, more than 5 million of Hy-Vee's customer's credit card and debit card information is now being sold on the dark web—an underground part of the internet accessed by an anonymizing browser and that is not indexed by search engines, where rampant illegal commerce occurs (e.g., buying and selling stolen card, subscription, and account information/credentials; buying and selling drugs, guns, counterfeit money)—through a well-known website called Joker's Stash, where the cache of stolen, for-purchase payment card information is listed as the "Solar Energy" breach.[11]

39. The card account records sold on Joker's Stash, known as "dumps," are being sold for prices ranging from $17 to $35 apiece. Buyers will receive a text file that includes all of

---

[9] HY-VEE, *Notice of Data Breach*, *supra* note 1
[10] *See id.*; KREBSONSECURITY, *supra* note 7.
[11] KREBSONSECURITY, *supra* note 7.

their dumps. Those individual dump records — when encoded onto a new magnetic stripe on virtually anything the size of a credit card — can be used to purchase stolen merchandise in big box stores.[12]

40. Although Hy-Vee did not initially confirm whether the Data Breach exposed credit and debit card numbers, cardholder names, and card expiration dates, the cache of data that is was being sold on Joker's Stash made clear that this level of information involving customers' credit and debit card information was certainly stolen from Hy-Vee as part of the breach.

41. After nearly two months of delay, on October 3, 2019, Hy-Vee published the Report on its website announcing additional details about the Data Breach.[13]

42. In the Report, Hy-Vee disclosed that it detected the Data Breach on July 29, 2019, which was carried out with the use of "malware designed to access payment card data from cards used on point-of-sale ("POS") devices at certain Hy-Vee fuel pumps, drive-thru coffee shops, and restaurants," which Hy-Vee revealed includes Hy-Vee Market Grilles, Hy-Vee Market Grille Expresses and the Wahlburgers locations that Hy-Vee owns and operates, as well as the cafeteria at Hy-Vee's West Des Moines corporate office.[14]

43. According to the Report:

> The malware searched for track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) read from a payment card as it was being routed through the POS device. However, for some locations, the malware was not present on all POS devices at the location, and it appears that the malware did not copy data from all of the payment cards used during the period that it was present on a given POS device.[15]

---

[12] *Id*.
[13] HY-VEE, *Hy-Vee Reports Findings from Investigation of Payment Card Data Incident*, *supra* note 4.
[14] *Id*.
[15] *Id*.

44. The Report also revealed that there were different timeframes for the Data Breach at Hy-Vee's different locations. Hy-Vee has identified the following:

> The specific timeframes when data from cards used at these locations involved may have been accessed vary by location over the general timeframe beginning December 14, 2018, to July 29, 2019 for fuel pumps and beginning January 15, 2019, to July 29, 2019, for restaurants and drive-thru coffee shops. There are six locations where access to card data may have started as early as November 9, 2018, and one location where access to card data may have continued through August 2, 2019. A list of the locations involved and specific timeframes are available below.[16]

45. In conjunction with publishing the Report, Hy-Vee has also posted an online tool allow customers to determine which location was impacted and during what timeframe.[17]

46. As is commonplace with payment card data breaches, the Data Breach was a result of malware that criminals routinely are known to use in payment card breaches. According to KrebsonSecurity,

> . . . typically, such breaches occur when cybercriminals manage to remotely install malicious software on a retailer's card-processing systems. This type of point-of-sale malware is capable of copying data stored on a credit or debit card's magnetic stripe when those cards are swiped at compromised payment terminals. This data can then be used to create counterfeit copies of the cards.[18]

47. Furthermore, neither the Notice, the Report, nor any statements issued by Hy-Vee give any indication as to the *actual* magnitude of the Data Breach, including confirmation of the number of stores actually targeted or the actual number of customers and cards affected.

48. Despite claiming to provide "additional details" through the Report about the Data Breach, the reality is that Hy-Vee has provided next to nothing by way of details surrounding the breach that would allow consumers to protect themselves against payment card fraud and identity theft.

---

[16] *Id.*
[17] *See id.*
[18] KREBSONSECURITY, *supra* note 7.

49. Although the Report indicates Hy-Vee "also notified federal law enforcement and the payment card networks,"[19] it is unclear whether Hy-Vee has reported the details of the breach to the Iowa Attorney General as required by Iowa law, Iowa Code § 715C.2.[20] Under Iowa law,[21] any data breach that affects at least 500 Iowa residents requires written notification to the Attorney General's Consumer Protection Division Director within five business days after notifying affected people.

Industry Standards and the Protection of Customer Card Information

50. It is well known that sensitive Card Information is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. At least 11 consumer companies reported data breaches in the last year. Many of them were caused by flaws in payment systems either online or in stores."[22]

51. Despite the known risk of a data breach and the widespread publicity and industry alerts regarding the other notable data breaches, Hy-Vee failed to take reasonable steps to adequately protect its computer systems from being breached, and then failed to detect the Data Breach for several months.

52. Hy-Vee is, and at all relevant times has been, aware that the Card Information it maintains as a result of purchases made at its locations is highly sensitive and could be used for

[19] *Id.*
[20] https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/2019 (last visited Oct. 4, 2019).
[21] https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications (last visited Oct. 4, 2019).
[22] Dennis Green and Mary Hanbury, "If you bought anything from these 11 companies in the last year, your data may have been stolen," BUSINESS INSIDER, available at https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited Apr. 2, 2019).

nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. Indeed, it used heightened data security technology at its grocery store, pharmacy, and convenience store locations, but not at the locations that were impacted by the Data Breach.

53. Its decision to utilize encryption at some of its other non-impacted locations, coupled with its explicit statements in its Privacy notice, makes clear that Hy-Vee recognizes the importance of adequately safeguarding its customers' sensitive Card Information. On its website, Hy-Vee's Privacy notice provides the following:

> **Privacy**
>
> **Our Commitment to Privacy**
>
> Hy-Vee, Inc. ("Hy-Vee", "we", "our" or "us") is committed to respecting and protecting our customers' privacy. . . . We take the issue of privacy very seriously and value the trust you place in us each time you visit our stores and use the services we provide.[23]

54. Hy-Vee is thus aware of the importance of safeguarding its customers' Card Information from the foreseeable consequences that would occur if its data security systems were breached.

55. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

56. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Hy-Vee to protect cardholder data, ensure the maintenance of vulnerability management programs,

[23] HY-VEE, *Privacy*, available at https://www.hy-vee.com/corporate/policy/privacy/ (last visited Oct. 4, 2019).

implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

57. The twelve requirements of the PCI DSS are: (1) Install and maintain a firewall configuration to protect cardholder data; (2) Do not use vendor-supplied defaults for system passwords and other security parameters; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (7) Restrict access to cardholder data by business need to know; (8) Identify and authenticate access to system components; (9) Restrict physical access to cardholder data; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel.[24]

58. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

59. Hy-Vee was at all times fully aware of its data protection obligations in light of its participation in the payment card processing networks and the stores daily collection and transmission of thousands of sets of Card Information.

60. Because Hy-Vee accepted payment cards containing sensitive financial information, it knew that its customers were entitled to and did in fact rely on it to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

---

[24] PCI SECURITY STANDARDS COUNCIL, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard Version 3.2*, at 9 (May 2016), available at https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1506536983345 (last visited Oct. 4, 2019).

61. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

62. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

63. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[25]

64. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses in regard to their data security obligations.

[25] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business* (Nov. 2011), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Oct. 4, 2019).

65. As noted above, Hy-Vee should have been and, based upon its use of encryption technology at certain locations, was aware of the need to have adequate data security systems in place.

66. Despite this, Hy-Vee failed to upgrade and maintain its data security systems in a meaningful way so as to prevent data breaches. Hy-Vee's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Hy-Vee are in stark contrast and directly conflict with the PCI DSS core security standards.

67. Had Hy-Vee maintained its information technology systems ("IT systems"), adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach.

68. As a result of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented restaurant and retail (and other) data breaches, Hy-Vee was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

69. Hy-Vee was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used recently to infiltrate large retailers such as, *inter alia*, Target, GameStop, Chipotle, Jason's Deli, Whole Foods, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Hy-Vee was aware that malware is a real threat and is a primary tool of infiltration used by hackers.

70. In addition to the publicly announced data breaches described above, Hy-Vee knew or should have known of additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland

Security, which alerted retailers to the threat of malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[26]

71. Despite the fact that Hy-Vee was on notice of the very real possibility of consumer data theft associated with its security practices and that Hy-Vee knew or should have known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols, and permitted massive malware intrusions to occur for months on end.

72. Hy-Vee, at all times relevant to this action, had a duty to Plaintiffs and members of the class to: (a) properly secure Card Information submitted to or collected at Hy-Vee's locations and on Hy-Vee's internal networks; (b) encrypt Card Information using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiffs and the class, which would naturally result from Card Information theft; and (e) promptly notify customers when Hy-Vee became aware of the potential that customers' Card Information may have been compromised.

73. Hy-Vee permitted customers' Card Information to be compromised by failing to take reasonable steps against an obvious threat.

74. In addition, leading up to the Data Breach, and during the course of the breach itself and the investigation that followed, Hy-Vee failed to follow the guidelines set forth by the FTC.

[26] *See* U.S. COMPUTER EMERGENCY READINESS TEAM, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (July 31, 2014) (revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A.

75. Industry experts are clear that a data breach is indicative of data security failures. Indeed, Julie Conroy—research director at the research and advisory firm Aite Group—has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[27]

76. The Data Breach is particularly egregious and its data security failures are particularly alarming given that the breach resulted in at least 5.3 million cards being stolen and illegally placed for sale on the dark web, and because the Data Breach was permitted to occur for over 6 months at some locations and over 7 months at others (with a handful of locations experiencing the breach for even longer). Clearly, had Hy-Vee utilized adequate data security and data breach precautions, the window of the Data Breach would have been significantly mitigated, and the level of impact could have been reduced, had the breach been permitted to happen at all in the first place.

77. One commentator in the data security industry noted as to a previous, unrelated data breach:

> . . . ***2 million cards on sale on the dark web would indicate this was a very successful project for the cybercriminals involved, and one which is likely to be incredibly profitable***. POS-malware breaches happen in the US with alarming regularity, and businesses should be well aware that they need to not only protect their central networks but also need to account for physical locations as well. . . . Moving forward, financial institutions should consider implementing a system of two-factor authentication in conjunction with a passive biometric solutions in order to mitigate the entirely avoidable outcomes of security incidents such as this.[28]

---

[27] Lisa Baertlein, "Chipotle Says Hackers Hit Most Restaurants in Data Breach," REUTERS (May 26, 2017), available at http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited Oct. 4, 2019).

[28] "Cyber Attack on Earl Enterprises (Planet Hollywood)," isBuzznews (Apr. 1, 2019), available at https://www.informationsecuritybuzz.com/expert-comments/cyber-attack-on-earl-enterprises-planet-hollywood/ (last visited Oct. 4, 2019).

78. With more than 5.3 million cards stolen in the Hy-Vee breach, this clearly marks a highly successful outing for criminals and a large failure on Hy-Vee's part as to data security.

79. As a result of the events detailed herein, Plaintiffs and members of the class suffered actual palpable fraud and losses resulting from the Data Breach, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Hy-Vee that Plaintiffs and class members would not have made had they known of Hy-Vee's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

80. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

81. For example, the Card Information stolen from Hy-Vee's locations can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.

82. To date, and as made clear in the Report, Hy-Vee is not taking any real measures to assist affected customers. In the first place, it has bled out information about the Data Breach at its own pace over the course of a few months, leaving victims of the breach in the dark and vulnerable to continued fraud. All that Hy-Vee has done to assist impacted is offer them some (quite obvious) sage advice: "It is always advisable to review your payment card statements for

any unauthorized activity. You should immediately report any unauthorized charges to your card issuer . . . ."[29]

83. These "suggestions" above make it clear that Hy-Vee is shifting the responsibility for the Data Breach to consumers, rather than taking real steps to assist its customers in protecting against the fraud to which it exposed them. Upon information and belief, to date, Hy-Vee is not offering credit monitoring or identity theft insurance to customers impacted by the Data Breach.

84. Hy-Vee's failure to adequately protect its customers' Card Information has resulted in consumers having to undertake various errands (e.g., obtaining credit monitoring, checking credit reports, etc.) that require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of their own money—while Hy-Vee is doing nothing to assist those affected by the Data Breach, and withholding important details about the Data Breach as it conducts its investigation. Instead, Hy-Vee is putting the burden on the consumer to discover possible fraudulent transactions.

CLASS ALLEGATIONS

85. Plaintiffs bring this action individually and on behalf of the following classes and subclasses (collectively referenced as "the class" herein) pursuant to FED. R. CIV. P. 23:

National Class

All individuals in the United States who had their credit or debit card information compromised as a result of the Hy-Vee data breach.

Illinois Class

All individuals in Illinois who had their credit or debit card information compromised as a result of the Hy-Vee data breach.

[29] HY-VEE, *Hy-Vee Reports Findings from Investigation of Payment Card Data Incident*, *supra* note 4.

Missouri Class

All individuals in Missouri who had their credit or debit card information compromised as a result of the Hy-Vee data breach.

86. Excluded from the class are Hy-Vee, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change, or expand the definitions of the class based on discovery and further investigation.

87. **Numerosity**: While the precise number of class members has not yet been determined, members of the class are so numerous that their individual joinder is impracticable, as the proposed class appears to include approximately 5.3 million members who are geographically dispersed. Upon information and belief, the Data Breach affected millions of consumers across the United States.

88. **Typicality**: Plaintiffs' claims are typical of the claims of the class. Plaintiff and all members of the class were injured through Hy-Vee's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other class member because Plaintiff and each member of the class had their sensitive data and Card Information compromised in the same way by the same conduct by Hy-Vee.

89. **Adequacy**: Plaintiffs are adequate representatives of the class because Plaintiffs' interests do not conflict with the interests of the class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the class will be fairly and adequately protected by Plaintiffs and their counsel.

90. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the class. The injury suffered by each

individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the class individually to effectively redress Hy-Vee's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

91. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to Plaintiffs and all members of the class. These questions predominate over the questions affecting individual class members. These common legal and factual questions include, but are not limited to, the following:

- whether Hy-Vee engaged in the wrongful conduct alleged herein;
- whether Hy-Vee owed a duty to Plaintiffs and members of the class to adequately protect their Card Information and to provide timely and accurate notice of the Data Breach to Plaintiffs and the class, and whether it breached these duties;
- whether Hy-Vee violated federal and state laws thereby breaching its duties to Plaintiffs and the class as a result of the Data Breach;
- whether Hy-Vee knew or should have known that its computer and network systems were vulnerable to attacks from hackers and cyber-criminals;
- whether Hy-Vee's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems resulting in the

theft of customers' Card Information;

- whether Hy-Vee wrongfully failed to inform Plaintiffs and members of the class that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard consumers' sensitive financial and personal data;
- whether Hy-Vee failed to inform Plaintiffs and the class of the Data Breach in a timely and accurate manner;
- whether Hy-Vee continues to breach duties to Plaintiffs and class;
- whether Hy-Vee has sufficiently addressed, remedied, or protected Plaintiffs and class members following the Data Breach and has taken adequate preventive and precautionary measures to ensure the Plaintiffs and class members will not experience further harm;
- whether Plaintiffs and members of the class suffered injury as a proximate result of Hy-Vee's conduct or failure to act; and
- whether Plaintiffs and the class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and the class.

92. Hy-Vee has acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the class, thereby making appropriate final injunctive relief and declaratory relief with respect to the class as a whole.

93. Given that Hy-Vee has engaged in a common course of conduct as to Plaintiffs and the class, similar or identical injuries and common law and statutory violations are involved and common questions far outweigh any potential individual questions.

94. The class is defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Card Information to cyber criminals due to Hy-Vee's failure to protect this information, adequately warn the class that it lacked adequate data security measures, and failure to adequately warn that it was breached. Class membership will be readily ascertainable from Hy-Vee's business records.

95. Plaintiffs reserve the right to revise the above class definitions and any of the averments of fact herein based on facts adduced in discovery.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

96. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

97. Hy-Vee collected Card Information from Plaintiffs and class members in exchange for its sale of food and other services at its impacted locations.

98. Hy-Vee owed a duty to Plaintiffs and the class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in Hy-Vee's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Hy-Vee's networks and data security systems to ensure that Plaintiffs' and class members' financial and personal information in Hy-Vee's possession was adequately protected in the process of collection and following collection while stored on Hy-Vee's systems.

99. Hy-Vee further owed a duty to Plaintiffs and class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

100. Hy-Vee owed a duty to Plaintiffs and class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiffs and class members whose confidential data Hy-Vee obtained and maintained.

101. Hy-Vee knew, or should have known, of the risks inherent in collecting and storing the financial and personal information of Plaintiffs and class members and of the critical importance of providing adequate security for that information.

102. Hy-Vee's conduct created a foreseeable risk of harm to Plaintiffs and members of the class. This conduct included but was not limited to Hy-Vee's failure to take the steps and opportunities to prevent and stop the Data Breach as described herein. Hy-Vee's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiffs and class members.

103. Hy-Vee knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Hy-Vee knew or should have known that hackers would attempt or were attempting to access the personal financial information in databases such as Hy-Vee's.

104. Hy-Vee breached the duties it owed to Plaintiffs and members of the class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiffs and members of the class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiffs and class members.

105. As a direct and proximate result of Hy-Vee's negligent conduct, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

106. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

107. Pursuant to the FTC Act, 15 U.S.C. § 45, Hy-Vee had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and class members' personal information.

108. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Hy-Vee, of failing to use reasonable measures to protect Card Information. The FTC publications and orders described above also form part of the basis of Hy-Vee's duty to protect Plaintiffs' and class members' sensitive information.

109. Hy-Vee violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Card Information and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Hy-Vee's conduct was particularly unreasonable given the nature and amount of Card Information it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers and financial institutions.

110. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security

measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the class.

111. Hy-Vee had a duty to Plaintiffs and class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and class members' personal information.

112. Hy-Vee breached its duties to Plaintiffs and class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and class members' financial and personal information.

113. Hy-Vee's violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

114. But for Hy-Vee's wrongful and negligent breach of its duties owed to Plaintiffs and class members, they would not have been injured.

115. The injury and harm suffered by Plaintiffs and class members was the reasonably foreseeable result of Hy-Vee's breach of its duties. Hy-Vee knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and class members to suffer the foreseeable harms associated with the exposure of their Card Information.

116. Had Plaintiffs and class members known that Hy-Vee did and does not adequately protect customer Card Information, they would not have made purchases at Hy-Vee's locations.

117. As a direct and proximate result of Hy-Vee's negligence *per se*, Plaintiffs and class members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Hy-Vee that Plaintiffs and class members would

not have made had they known of Hy-Vee's careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

118. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

119. Plaintiffs and class members who made purchases at Hy-Vee's locations during the period in which the Data Breach occurred had implied contracts with Hy-Vee.

120. Specifically, Plaintiffs and class members paid money to Hy-Vee and, in connection with those transactions, provided Hy-Vee with their Card Information. In exchange, Hy-Vee agreed, among other things: (1) to provide food, gasoline, and food services to Plaintiffs and class members at its various locations; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and class members' Card Information; and (3) to protect Plaintiffs' and class members' personal information in compliance with federal and state laws and regulations and industry standards.

121. Protection of personal information is a material term of the implied contracts between Plaintiffs and class members, on the one hand, and Hy-Vee, on the other hand. Indeed, as set forth, *supra*, Hy-Vee recognized the importance of data security and privacy of customers' sensitive financial information in the privacy policy. Had Plaintiffs and class members known

that Hy-Vee would not adequately protect customer Card Information, they would not have made purchases at Hy-Vee's locations.

122. Hy-Vee did not satisfy its promises and obligations to Plaintiffs and class members under the implied contracts because it did not take reasonable measures to keep their personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

123. Hy-Vee materially breached its implied contracts with Plaintiffs and class members by failing to implement adequate payment card and Card Information security measures.

124. Plaintiffs and class members fully performed their obligations under their implied contracts with Hy-Vee.

125. Hy-Vee's failure to satisfy its obligations led directly to the successful intrusion of Hy-Vee's computer servers and stored Card Information and led directly to unauthorized parties access and exfiltration of Plaintiffs' and class members' Card Information.

126. Hy-Vee breached these implied contracts as a result of its failure to implement security measures.

127. Also, as a result of Hy-Vee's failure to implement the security measures, Plaintiffs and class members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

128. Accordingly, Plaintiffs and class members have been injured as a proximate result of Hy-Vee's breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILL. COMP. STAT. §§ 505/1, *et seq.* ("Illinois CFA")
(On Behalf of Plaintiff Perdue and the Illinois Class)

129. Plaintiff Perdue incorporates all foregoing substantive allegations as if fully set forth herein.

130. Plaintiff Perdue and the class are "consumers" as that term is defined in 815 ILL. COMP. STAT. § 505/1(e). Plaintiff Perdue, the class, and Hy-Vee are "persons" as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

131. Hy-Vee is engaged in "trade" or "commerce", including provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

132. Hy-Vee engages in the "sale" of "merchandise" (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

133. Hy-Vee engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including but not limited to the following:

- failing to maintain sufficient security to keep Plaintiff Perdue's and class Members' sensitive Card Information being hacked and stolen;
- misrepresenting material facts to the class, in connection with the sale of goods and services, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard class members' Card Information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the class, in connection with sale of goods and services, by representing that Hy-Vee did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of class members' Card Information; and

- failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect class members' Card Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

134. In addition, Hy-Vee's failure to disclose that its computer systems were not well-protected – including Hy-Vee's failure to disclose that, despite the general trend of a shift to chip technology for point of sale transactions, Hy-Vee had not made this transition – and that Plaintiff Perdue's and class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Hy-Vee knew such facts would (a) be unknown to and not easily discoverable by Plaintiff Perdue and the class; and (b) defeat Plaintiff Perdue's and class members' ordinary, foreseeable and reasonable expectations concerning the security of their Card Information on Hy-Vee's servers.

135. Hy-Vee intended that Plaintiff Perdue and the class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Hy-Vee's offering of goods and services and incorporating Plaintiff Perdue's and class members' Card Information on its servers, in violation of the Illinois CFA.

136. Hy-Vee also engaged in unfair acts and practices by failing to maintain the privacy and security of class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

137. Hy-Vee's wrongful practices occurred in the course of trade or commerce.

138. Hy-Vee's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Hy-Vee that applied to all Class members and were repeated continuously before and after Hy-Vee obtained sensitive Card Information and other information from Plaintiff Perdue and class members. All class members have been adversely affected by Hy-Vee's conduct and the public was and is at risk as a result thereof.

139. Hy-Vee also violated 815 ILCS 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et. seq.*, which provides, at Section 10:

> Notice of Breach.
>
> (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

140. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

141. As a result of Hy-Vee's wrongful conduct, Plaintiff Perdue and class members were injured in that they never would have allowed their sensitive Card Information – the value of which Plaintiff Perdue and class members no long have control – to be provided to Hy-Vee if they had been told or knew that Hy-Vee failed to maintain sufficient security to keep such data from being hacked and taken by others.

142. Hy-Vee's unfair and/or deceptive conduct proximately caused Plaintiff Perdue's and class members' injuries because, had Hy-Vee maintained customer Card Information with adequate security, Plaintiff Perdue and the class members would not have lost it.

143. As a direct and proximate result of Hy-Vee's conduct, Plaintiff Perdue and class Members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Hy-Vee that Plaintiff Perdue and class members would have never made had they known of Hy-Vee's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

144. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiff Perdue and the class seek actual damages, compensatory, punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Hy-Vee's violations of the Illinois CFA.

COUNT V
Violations of the Illinois Uniform Deceptive Trade Practices Act
815 ILL. COMP. STAT. §§ 510/1, *et seq*. ("Illinois DTPA")
(On Behalf of Plaintiff Perdue and the Illinois Class)

145. Plaintiff Perdue repeats and realleges the allegations above as if fully set forth herein.

146. Plaintiff Perdue, the Class, and Hy-Vee are "persons" as defined in 815 ILL. COMP. STAT. § 510/1(5).

147. The Illinois DTPA broadly prohibits deceptive trade practices. As set forth herein, Hy-Vee failed to safeguard Plaintiff Perdue's and class members' confidential and sensitive personal information. Accordingly, Hy-Vee has engaged in deceptive trade practices as defined in 815 ILL. COMP. STAT. § 510/2.

148. Hy-Vee's actions as set forth above occurred in the conduct of trade or commerce.

149. Hy-Vee knew or should have known that its conduct violated the Illinois DTPA.

150. Hy-Vee's conduct was material to Plaintiff Perdue and the class.

151. As set forth herein, Plaintiff Perdue and the class suffered ascertainable loss caused by Hy-Vee's violations of the Illinois DTPA, which proximately caused injuries to Plaintiff and the other class members.

152. Pursuant to 815 ILL. COMP. STAT. § 510/3, Plaintiff Perdue and the class are entitled to an award of injunctive relief to prevent Hy-Vee's deceptive trade practices and, because Hy-Vee's conduct was willful, an award of reasonable attorneys' fees.

COUNT VI
Violation of the Missouri Merchandising Practices Act
MO. ANN. STAT. § 407.020(1), et seq. ("MMPA")
(On Behalf of Plaintiff Murray and the Missouri Class)

153. Plaintiff Murray repeats and realleges the allegations above as if fully set forth herein.

154. Plaintiff Murray, the Class, and Hy-Vee are "persons" as defined in MO. ANN. STAT. § 407.020(1).

155. The MMPA provides in part:

> The act, … by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or

> omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce … is declared to be an unlawful practice.

MO. ANN. STAT. § 407.020.

156. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Personal Information of Plaintiff Murray and class members, Defendants violated the provisions of § 407.020 of the MMPA.

157. Defendants' actions as set forth above occurred in the conduct of trade or commerce.

158. The acts and conduct of Defendants as alleged above violated the MMPA by, among other things:

- failing to maintain sufficient security to keep confidential and sensitive financial information of Plaintiff Murray and class members from being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of goods and providing online purchases services, by representing that Defendants would maintain adequate data privacy and security practices and procedures to safeguard class members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the Class, in connection with the sale of goods and providing online purchases services, by representing that Defendants did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of class members' personal information; and,
- failing to prevent the Data Breach and promptly notify consumers thereof, failing to maintain the privacy and security of class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws.

159. Due to the Data Breach, Plaintiff Murray and class members have lost property in the form of their Personal Information and have suffered actual damages. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding the

confidential and sensitive financial information of its customers has resulted in Plaintiff Murray and class members spending time and money to protect against identity theft. Plaintiff Murray and class members are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

160. As a result of Defendants' practices, Plaintiff Murray and class members have suffered injury-in-fact and have lost money or property. As a result of Defendants' failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Plaintiff Murray and class members have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

COUNT VII
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

161. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

162. This claim is plead in the alternative to the above implied contract claim.

163. Plaintiffs and class members conferred a monetary benefit upon Hy-Vee in the form of monies paid for the purchase of food and food-related services at its locations.

164. Hy-Vee appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and class members. Hy-Vee also benefited from the receipt of Plaintiffs' and class members' Card Information, as this was utilized by Hy-Vee to facilitate payment to it.

165. The monies for food, dining, and food-related services that Plaintiffs and class members paid to Hy-Vee were supposed to be used by Hy-Vee, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

166. As a result of Hy-Vee's conduct, Plaintiffs and class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and class members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

167. Under principals of equity and good conscience, Hy-Vee should not be permitted to retain the money belonging to Plaintiffs and class members because Hy-Vee failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

168. Hy-Vee should be compelled to disgorge into a common fund for the benefit of Plaintiffs and class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a) and (b)(3), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiffs as class representatives and their counsel as class counsel.

B. Award Plaintiffs and the class appropriate monetary relief, including actual damages, restitution, and disgorgement.

C. Award Plaintiffs and the class equitable, injunctive and declaratory relief as may be appropriate. Plaintiffs, on behalf of the class, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly class members who are more susceptible to fraud and identity theft.

D. Award Plaintiffs and the class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiffs and the class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiffs and the class such other favorable relief as allowable under law or at equity.

Dated: October 15, 2019

Respectfully submitted,

/s/ Kyle Shamberg

CARLSON LYNCH, LLP
Katrina Carroll
Kyle Shamberg
111 W. Washington Street, Suite 1240
Chicago, IL 60602
Phone: 312-750-1265
Email: kcarroll@carlsonlynch.com
Email: kshamberg@carlsonlynch.com

Benjamin F. Johns (PA Bar No. 201373)
Andrew W. Ferich
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue

Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
awf@chimicles.com

Cornelius P. Dukelow
Oklahoma Bar No. 19086
Abington Cole + Ellery
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com
www.abingtonlaw.com

Counsel for Plaintiffs and the Putative Class